Stéphane Duguin □
Patrice Riemens /
Caterina Riva *

/ Shall I open-

* Yes, please.

/ This interesting discussion.

We're looking at each other, who is going to start. So I guess the decor is not visible for whoever is listening to us, but it's quite interesting to be in the underground of the museum and my name is Stephane Duguin. I'm the chief executive officer for the CyberPeace Institute in Geneva. I've been told to give some words of background.

So I'll start like this quickly civil servant for most of my career with I would say after so many years, we can say an obsession of supporting victims of crime and now the crime is in the cyberspace. So that's what I do for a living and helping the one, the most vulnerable against the worst of the attack, and I guess we can start with that.

* Great. I'm Caterina Riva and I am maybe the odd one out with the word we're discussing together tonight, which is hacker. So I'm going to give a little autobiographical introduction. I'm currently the director of a museum in Termoli, Southern Italy called MACTE Museo di Arte Contemporanea di Termoli. I've been there for a year. So with the challenges of what the last year has been. Before then, although I'm Italian, I worked and lived abroad. I was in Singapore for two years. I was working for the Institute of Contemporary Art Singapore, whose acronym is ICA. It's really funny because if you do a quick Google search on ICA Singapore, it sends you to the link of the immigration authority. So, and I think also when I first arrived, I made a mistake of linking, I don't know, my social media to that and then someone pointed out that I was redirecting maybe to where I didn't want to be.

Also those two years in Singapore, I have to say they really changed my outtake on how digital life has been changing everything. In particular, trying to address how it's changing the production of artworks and how artists and curators work. Also, being in Singapore, I experience firsthand a kind of, I guess, constrictive government and technological experiments being taken out on population. So that made me a little bit scared as a citizen of the world. Also before Singapore, I spent three years in Auckland, New Zealand as the director of a contemporary art space called Artspace, which again was a really interesting opportunity to encounter a very far away and very layered post-colonial community. That taught me a lot about being elsewhere and working with different audiences and maybe challenging our Eurocentric ways of thinking.

Going back a little bit more in time, I studied and worked in London where I did an MFA in curating at Goldsmiths and I, at the same time, I opened up a curatorial project space with two colleagues called FormContent and we did projects there in real life and we had a website but maybe things weren't as dematerialized as they seem to be now.

Maybe before passing on, I just would like to say that maybe I'm here also to learn, maybe bring my own kind of outsider look and perspective to the conversation.

□ Hi, my name is Patrice Siemens. If Caterina is odd person out, I may be the odd person in with emphasis on odd because I'm supposed and considered to be a hacker. My background is very simple. I've been academic for the greatest part of my life. I'm a geographer but I switched quite early from geography into the electronic networks as it was called in the time, which became for the general public, the internet, which is much older than many people believe, because many people would date the Internet from the '90s and maybe even later. Anyway, I became Internet and especially cultural internet activist. I have been part of many events, generally in a peripheral position because I don't like to be at the top of things. I'd say I much prefer to be a kind of observer. Maybe is the most important thing for now since the theme is hacker, is that I might surprise people in the sense that I am, as I often say, a hacker, but I am not a coder.

And the most important point that I want to make because it is in my opinion the beginning of a lot of misunderstanding: however hackers are very much connected to information and communication technology as it is called or say the Internet, the electronic networks and the technology which supports it all, it is my view and also the view of, I am happy to say, quite a number of hackers, that connection to IT is never a necessary and especially not a sufficient condition to be a hacker. To be a hacker is a question of, again, in my view, of attitude and of ways of doing things. I will start the conversation by saying that the main characteristic of somebody who will be considered a hacker is to be curious. That curiosity is the most important thing. A lot of things goes with it, with always keeping in mind that as a proverb say, "curiosity killed the cat."

* Great. I wonder if we want to establish some kind of ground for what a hacker is or if we want to jump in other directions. Because there is the standard definition, but I'm personally quite interested in the characterization or should I say of the miss-characterization of this figure and this kind of disembodied nature being one of the main points. I wonder if you can help me understand the basic difference between a hacker and a 'cracker', if there's a different attitude, as you say, Patrice.

□ Well, when you are talking about misunderstanding, maybe the most important one, in the olden days of quite early on, there was this differentiation made between a hacker and a cracker. A hacker is a good person or a 'white hacker'. A cracker is a bad person doing bad things, which you should be combating. In my view, it is, as quite often, it is absolutely simple, a cracker is not a hacker. The hacker works according to the hacker ethic, which is quite well defined and which says, "do no harm".

In the beginning time of hacking... Well first maybe it's good to know that the word hack and hacking, which apparently, but I'm not very sure of that, but apparently originated in the MIT the Massachusetts Institute of Technology. Hacking then meant just coding, it was just about making computer works.

Which at that time was really a kind of pioneering activity with very little being already known, you were creating knowledge as you were going, that was a very important feature, that knowledge was absolutely open. It was shared and it was open.

The Internet came out of that and one of the maybe most crucial problem of the Internet as we know it today is this, you would almost say, it is its original sin that it was open and that it was built to be open. When all kind of bad things started to happen of which crackers are part, but also the commercialization and financialization of the internet and trying to make things secret again was always a kind of desperate reaction, you can use all kind of metaphors for it like, call it: mopping up the floor while the tap is open and a lot of water is flowing in.

So hackers in the beginning were simply coding and then it evolved. It also very important reason is that MIT saw this happening, the open knowledge being closed in. It became closed in for various reasons, the most important one being commercialization and commerce is of course based, I think wrongly - but it's the way it works on secrecy.

/ Yeah.

□ On property knowledge.

/ IPR.

□ You want to explain it?

/ No, no, just no, just what you're saying on IPR, I mean the basis of commerce.

□ Exactly, IPR is exactly what hackers are coming into conflict with. The second thing, what hackers are doing is gaining access. If the thing is open you don't have to try, gaining access is easy. You just take avail of the access, but if it's closed, you have to gain access in some way or another. Then they say the problem started when hackers were gaining access illegally. Illegally because what they wanted was to gain access to networks that were closed. Then quite early in the beginning, kind of a war say or conflict started to happen between hackers and network administrators.

Young people were at it, generally at that time hackers were really very young. I was with Dutch hackers since the beginning, well, almost the beginning. They started outside Amsterdam, which is quite remarkable in itself because in the Netherlands, everything is supposed to happen in Holland. And with in Holland everything is supposed to happen in Amsterdam, but they came from a bit north and they were 15, something like 15, 16 years old. They came to the open, to Amsterdam by the way, they were by then something like 19, 20 years old. That's when I joined them, a bit by accident. They interacted with... Their main aim was to gain access to electronic networks which were closed.

At that time these were government networks, academic network. Commercial networks were coming in also, but I think an important point is that commerce came into the internet relatively late.

One of the things Bill Gates is rumored to have said that the internet was a fad and it will pass away like so many things. Well, you see where we are now. So in the beginning when the Dutch hackers came into the network, they were combated for a part, but also admired by, and they got quite early access on agreement with the main academic network, and from there on, at least in the Netherlands, the kind of more modus vivendi came into being. I am speaking of the very late ‘80s and early ‘90s, by the way. In Italy, for instance, things were completely different. Hackers from the beginning were seen as an evil force. In Italy they were also much more radical politically speaking, than they were in the Netherlands.

So in Europe, generally as far as hackers are concerned, you can make a difference between the north and the south. In the center, the south was early politically militant and got into really stiff repression from the state. Whereas in the north a kind of compromise evolved, in the Netherlands especially because we had a very early on a computer criminality laws. At which stage the hackers profiled themselves as social movement. By profiling themselves as a social movement, they became bit unassailable.

Because you can’t touch social movements. Social movements are okay. So as long as they were not engaging in criminality, that was quite all right. To come back to: What are hackers doing? There are several stages in what hackers are doing for instance, they may be acting like criminal hackers in helping to make systems secure. This is a very positive, quite often, not very much acknowledged, also very difficult to acknowledge, activity because unless there have been hired in by the institution, company or government or whatever, indeed, to probe their network for failures, for what you call it for-

/ Vulnerabilities.

□ Exactly vulnerabilities. If they do it by themselves and then signal to the instances that they have this and that vulnerability. Nowadays, there is some kind of protocol for that but in the early days, it was really kind of, “Oh, bad weather is coming. Let’s smash the barometer!” or, “This messenger is telling me my armies have been smashed up. Let’s kill the messenger!” Lot of difficulties arose out of that attitude.

And then yes, we were provided with a few key words Lara. Lara, the artist, suggested words like: phishing, spam, ransomware. I am not really, to put it bluntly, I am not very interested in that aspect of things. That does not represent a hacker activity for me. That is a criminal activity, making wrong use of computers while having a knowledge, which is unfortunately the same knowledge as what real hackers have of systems. I am much more interested in that aspect of the knowledge.

Because to me one of the major aspect of being a hacker, and that's not only valid for IT, it is valid for technology in general and for knowledge in general, a hacker is someone having the possession of an illegal, or let me say, unauthorized knowledge. In a certain sense, we are back in the Egyptian times. The high priests have the knowledge, they are the ones authorized to have it. Anyone else with that knowledge is by definition a criminal, and I like to end here.

/ No that's... I mean, you said a lot and that's very interesting. I'll start with the end when you said knowledge. I mean, that's to me hacking, at least how I understand this, and I guess I'm the vast majority of people looking topic, understand this. First, there's no negative connotation to the word. When in fact we're talking about criminals, but for me, it has nothing to do with hacking. For me hacking is really something it's about knowledge, that is about empowerment of citizen to understand the system to interact with. We are interacting with a system. We are interacting with an ecosystem. We should be a human being in capacity to understand what is happening, how it works, and if it doesn't work to our interest to make it better.

And that was really at the source of the philosophy, because it's really going towards the philosophy, the hacking. It's a way of life. The way of seeing your environment though, have been critic about your environment. To me, linked to hacking, there's a lot of high sense of self critic, defense against manipulation, defense against factory of information that is trying to make you act in a way that you don't even know why you are acting like this. Hacking it's about going against that. So keeping your brain up and trying to look into the cracks in between the code.

Something that you said, and I absolutely subscribe to this, then, whatever else you do using a computer, using a knife, using a car, using a bomb, using whatever, it's crime, but it has nothing to do with hacking. So that would be the same that you would say that I don't know, a race driver is a nice person when he is driving a race. When someone is using a car to break the rules on the road, so that leads a criminal, and then we have to define this. Because the car is the same car. No, this doesn't make any sense.

Something that you mentioned also about power. You didn't mention power, but it led me to think about power and knowledge because, I don't remember who it was, I think it was Zimmermann, but help me there. I don't want to say a nonsense, but if people are listening to us, they will correct-

□ Sure.

/ I think it was Zimmermann who the first time put in place the PGP. At the moment where this was known from his friends, from his network, they told him, "Watch out, because for sure the FBI is going to come on you because what you're doing now is nothing illegal, but because you're doing it and it was supposed to be something that was owned by the states" says who, the states, "then something is going to happen to you." No surprise. The FBI came there.

When today decades after that, encryption is at the basis of all the services that we have on internet. Without encryption, we cannot secure the exchange in finance. We cannot secure the… I mean, I don’t have to explain why it’s so important. So it’s a question of momentum. If at that time, that person with a hacker philosophy state of mind and approach would not go into the boundaries of I want to make sure that the encryption become a probably good, then maybe this would never have been happening for the vast majority of us. So at some point you need to play, as you were saying with the boundary, with the rules and to be there. But if you do this for knowledge, if it’s transparent, if it’s open, if it’s really for the common good, if you don’t do this for ego, and to prove that you’re better than the system and you want to beat something, because sometimes it also can go there. As long as we don’t mix this with crime, and it’s quite easy to define crime, so maybe it’s more complicated to define hacking, but it’s very easy to define crime. So maybe-

□ Yeah.

/ It’s easier to go there. That’s where I see at least this in my… in my mind construct, I think.

□ The interesting point about encryption is that you first had a stage where you were fighting for the right to encrypt. And nowadays we have the stage basically in my mind, came in after 9/11 you have to fight for the right to decrypt.

/ Yeah, I mean, we can talk about this, but this is… You opened a lot of very good conversations. There’s one about encryption. There’s a one about vulnerability, scanning and bad bounty when in some countries, if you do this, you’re still criminalized and you even have to have the permission, to make sure that you’re going to detect every vulnerability in a system that if it exploit is going to trigger the mass surveillance of million of people. And because you’re looking into that, you need to ask, “Sorry, can I have the permission, please don’t put me in jail.” So it’s kind of a crazy situation. Encryption is the same, I mean, but okay. We can discuss about this afterwards. We’re happy to come back to it.

* I think there are so many interesting things on the table. I’m really interested as well in this question of ethics that I think you also are both really interested in. Maybe one way we can go about this is also open a more geopolitical kind of landscape, because I realize we often make the mistake of thinking as you know, one word, one internet, but things do change quite drastically, depending on which point interview you look at them from. I’m also thinking of kind of very simple artistic examples as well. For instance Aaron Schwartz.

I’m sure you are familiar with his name, when he was still alive, he was commissioned to propose an artwork with another New York based artist called Taryn Simon. And they came up with this quite interesting index of the same words in different regional contexts. How it is visualized on browsers in different places so let’s take the word ‘peace’.

I don't have the visual reference on me now, but for example is a dove with an olive branch in one country. It's a woman with a flag in another one, depending on religious, gender rules, etc.

The other aspect I'm super interested in, and to me is a crux in this discussion is digital surveillance: what's happening to us is linked to the idea of obfuscation. To me power lies with the ones that know how to use certain things. All the rest of us are left with clicking blindly on cookies because we are too tired to read the fine prints. That's how things are gradually taken away from our understanding and our knowledge.

Because you can think something and name it, but also you can make stuff happening without most of the people understanding how it works. Another thing I'm really interested in is the idea of the body and how, when we try to imagine what a hacker is or does, we never think about the social movement or a person trying to do something. It's always looked at through the lens of data and money or something quantifiable. Maybe also the ways it is wrongly portrayed in the media. Going back to what you were mentioning about Lara Favaretto, the artist that invited us and whose project Thinking Head Clandestine talks, she sent a series of images to inspire us or for us to consider.

They were very loose and maybe not necessarily linkable to this idea of hacker, but there was one that to me was kind of interesting and it was this man whose face you couldn't see and had like a jacket over his head, as if he didn't have a head and was headless for some reason. I'm just going to put it out there.

□ Sounds like the idea of a hacker in the mainstream media.

* I know. Yeah.

/ That, that guy with the hoodie that's-

* Yeah. Mr. Robot.

/ That is the one doing the bad thing all over the world. Yeah. Interesting figure for sure. I mean, while we think this is the hacker it gives a lot of space for the entities that are really doing a big harm on the internet to be unchecked. I mean, it's easier to give a scapegoat, easily identified, more or less young, more or less marginal. And that's the person that is the threat of the internet.

□ That's on, say, maybe at the meta level, that's the whole problem of unauthorized knowledge. The holder of an unauthorized knowledge is going to be the scapegoat because the holder of the unauthorized knowledge is not doing what the ones with the authorized knowledge are doing. And that is where the harm is. And you are completely right to say that the ones doing the most harm to the internet or to society in general.

/ To the population, exactly.

□ To society in general is… I mean, it's very necessary to take a lot of our conversation out of IT, out of the technology to project it to society in general. And one of the main mover of that is, of course… But naming it is immediately killing the conversation, almost, is to speak out the C word, for Capitalism.

/ Yeah. That's true. Because the… Yeah. No, it's very true. So just react on something that you were just saying, the why, I mean, a personal level I've been interested to, to join and lead the CyberPeace Institute. It was because of CyberPeace it's not a cybersecurity institute. You know, it's not about securing the computers and the networks, etc. It's okay. It's important, but that's not, that's not what I would strive for. What's interesting here is to say this internet, this type of space where I want to call it, this kind of mental construct, because doesn't really exist, in fact. It's just a mean to an end. And the end is the safety, the security, the dignity, the equity of human beings. In whatever they do, and what they do can be very critical.

I mean, without a secure cyber space today, you don't have access to water. You don't have access to food, you don't have access to healthcare. You can't discuss, you can't get knowledge. And you are saying it depends on the region of the world where you are in the countries. This is a specific meaning if you're in the Western world, because everything is digitize and you click and something happens like the magic of three centuries ago. But if you're other part of the world and you want to access this, it's not via the internet that you're going to access it. You're going to access it, there are capitalist services that are going to pretend to be the internet. And that's problematic.

□ Yeah, it is very one of the most shocking things. And I admit that I did not realize that because it is so obvious. And then think that I was in development studies! Can you imagine? But yes you are absolutely right in saying that we have to, we have to look at other parts of the world. When I read that the failure of Facebook, which was a few days ago if I'm not mistaken, put us users of Facebook, of which I'm not, into major inconvenience, because it was their lifeline via WhatsApp. It was a lifeline for people. And that was absolutely shocking to me on two planes. Yeah, it's a scandal that a failure of Facebook put people into real life difficulties. But it's also a scandal that it has come to that. Why is it that people have become so dependent on proprietary technologies, which are not made for their interest in mind, but only to make money out of it? By the way, I never understood how you can make money by giving free services to people who have no cash anyway.

But that's completely another point. That's my own naivety and un-knowledge. But you have that term, proprietary knowledge, which is bad in itself at that level. That's one of the thing we should combat. But yeah that is one of my many problems. Stephane is in a better position than I am, because at least he has a focus in an institution which is focusing on something quite precise, even if it is very wide. But if you are like me an observer of what is going on in general, you are looking at failures all over the place.

And then I'm not even talking about the general 'clusterfuck' society is in: climate for instance. Climate? Finance?

* It goes back to the big C. Stèphane, would you like to tell us a bit more about the CyberPeace project? I really like this title. And I was also thinking how usually these conversations are framed are around binaries and maybe a good way of trying to move past this is enlarging the terminology and from a very negative space, bring it to something potentially positive. And I was imagining *War and Peace*, the novel, you're theCyberPeace of that equation, maybe. Do tell us more about how you got there.

/ My pleasure with... Something that you said before in fact was interesting. When I joined, it was before that was in my year in Europole. Before in Europole, I was program manager to create and then be chief of staff for the European Cyber Crime Center. And then I created and led the unit that was anti Daesh and Al-Qaeda propaganda on-line in between Charlie Hebdo and Bataclan when it was really like something. Yeah, it was quite tragic. And despite the fact that all of this is happening and is impacting human beings, it's a fact, I guess, everyone knows what everyone has. The hint of it. I was thinking of your Google, search. You know, that you're doing different parts of the world. If today you make a search and you take the big names of the big cyber attacks. So you take WannaCry, NoPtr, Kaseya, SolarWinds. First, you need to know what they are.

So it's really a cluster of knowledge. So you need to be a bit informed to understand that this could, you could be a victim of something, not even know the name of. So let's start with that. But imagine that you know, you put that in Google, in Bing, in Wherever.go. What you're going to see, images. Are images of computer. You'll see figures. You'll see like numbers of cache that has been stolen etc. What you will not see ever is the face of someone as if this is computer fighting computers. It's the network hitting the network. And this is so non humanized as a problem. So how can we, how can we hope to design human-centric solutions? And that's really what yeah decided me to join the institute, because it was a practical vehicle to implement human-centric solution towards vulnerable communities.

What we do, we provide assistance to the one with the least capacity to defend themself against the one that have money, time, incentive, network to attack. And when the symmetry is at the worst, that's where we enter into play. And for example, we specialize ourself in helping NGOs. So NGOs in humanitarian sector, where their mission is sensitive, their field of action is sensitive, their data is super sensitive, their beneficiaries is super sensitive, and the cybersecurity level is very, very low. And criminals know that, state actors know that, but there was no one really to defend them. So that's where we want to spend our resources and try to make a difference. But not only to have like transactional help, because it's nice to help people. I mean, it's what you need to do. But the whole idea is how the knowledge that you generate from that help, what are the cracks? What are the vulnerabilities? Who are the real actors, who are the real threats?

He's not that guy that everyone is looking for with his hoodie in his basement. That's not this one. So it's state actors, it's the hybridization between criminal groups and state actors. These are the real threats. And how do we make sure that states when they discuss about norms and law and regulation, when they pave the way of the future of you, me or cyberspace, the ones for the future generation. How do they understand where the real threat is? But not starting to put text to treaty on the basis of, "Oh no, no no, but we know who is the cyber criminal. He's the hacker. He's the one that doesn't like the black box. He's the one that is not happy and okay. Smiling when he's clicking and scrolling down with algorithm." He or she has no clue how they work. I guess we can be a bit more ambitious for-

✱ And maybe it's about also turning the lens and showing the effects or the people affected by this rather than the supposed culprit. What might help, in my mind, is getting less abstract and lead by examples. So I don't know if you want to share, real events. I just wanted to add something because you were mentioning when there was a big freeze of the social media. It's very layered conversation and as people in the West with a certain level of education and access to things we can decide to log off Facebook. But for most people that use WhatsApp is survival like talking to their family back in Africa when they live and work in Europe or elsewhere and it's a tool. So they don't even question what's behind it.

□ By the way, I find that very problematic that we have landed in a situation like that. I would just like to come back to what you said about when government are enacting rules and etc. One of the biggest problem I think is the very limited, sometimes non-existent knowledge of rule makers, of decision takers, of how the technology works. The technology has become, in fact, completely out of control. And one of my main contention and it has at least a lateral connection to people using WhatsApp in quote/unquote developing countries. That is that technology has escaped, even I think in some instances, the control of the people developing it and using it. I see a bit of parallel with the financial crisis: when the financial crisis happened in 2008, the diagnostics were some were about: how could it come?

And so, and then one discovered that a lot of things, a lot of financial instruments were not even understood, the workings of financial vehicles were not even understood by the people who were acting on them. It was a kind of rush forward and tech and IT, information technology, in my view, has gone the same way. So there's also a big problem there. So empowering people is probably not enough in empowering for the situation we have now. We might also be thinking about reversing the situation in the sense that the technology, as it exists now, has become really a bit too complicated. You cannot simplify technology to the utmost limit. One of the example I have is that my friend, now disappeared, Arjen Kamphuis, was an expert in Internet security and in encryption, and he was really propagating the use of encryption by vulnerable people.

In his case, and that was mostly in the West, it were journalists advocate human rights and people like that.

But when it comes to propagating this encryption for everyone there was one big problem: you cannot simplify encryption endlessly, yet the average user will not understand it up to even the minimum level that you have to understand it. So you have a gap between the absolute minimum you can reach in complexity, and still understandable complexity of encryption, and the maximum average of knowledge attained by the majority of the users. And that gap for the time being is unbridgeable. And that is something that you will see in many instances.

* But the gap is getting larger.

□ That I cannot say. I found the image good enough, without the need to quantify it. It's of course, very important to know whether the gap is widening or diminishing because, especially if it diminishes, then you can hope that you will reach a point that there is security for everybody, the end of vulnerability. The end of the problems that have vulnerable peoples and communities, which you are addressing, which Stephane is addressing can be closed. But if it is augmenting, which might very well be the case. Well, in that case, yes-

* It depends from which perspective you're looking at this from. The big C corporations or the people, certain groups.

/ What you were saying before, in terms of the lack of digital literacy in the policy maker sphere. It's very true. It's very, very true. I mean, in my years in Europole or in work with the CyberPeace Institute I spent, and we spent, a lot of time providing knowledge to policy makers and it's not about the position or it's about the basic knowledge, the keys that you need to have to understand the technology, that the topic that you've been presented. And that's quite tough also because this, especially in policy making, the knowledge is not existing in the vacuum, it's existing in a context of an organization. The way government are organized is putting a frame on what they're supposed to understand, what they're not supposed to understand. The topic they're supposed to look into, they're not supposed to look into. The silos that are existing therefore decades. And you will not...

Very recent example. You wanted example. So you have discussion at United Nation on cyber security. So you have groups, United Nation groups, two of them already. So interesting. Open in a working group and group of experts. Okay. Let's go beyond the acronyms. United Nation discussion to discuss about norms and regulation in the cyberspace for responsible behavior. You're part of that. Then you have another initiative with a UN cybercrime treaty where there, this is about the future of how to understand cybercrime and how to fight cybercrime. It's not the same group. And when you discuss with ministry of foreign affairs, and I am doing this a lot, telling to them at the end of the day you know behind, this is the same internet, it's the same cables. What you need to learn is more important is the difference between the lower level of the internet when you're really close to the cable, almost at electrical level, and when you are on the content that is passing by the pipelines. Because then suddenly it's a different topics that you organize yourself alongside this would make sense.

That by default, you consider that, “This is me. This is me. And you know, we never worked together. And that’s the way it is.” And because you organize like this, you frame the topic and you absolutely blind to the reality of the technology, what it says, then there’s an issue.

The second gap, you are asking another example, is this reflex specific government that someone needs to be responsible. Point me to the responsible community. Is that the industry? Is this the criminals? Is this in other states? Who should I investigate? And let’s take the example of Deepfakes. So I was still in Europole at the time, end of 2017, when Deepfakes become a bit mainstream. How it became mainstream.

It’s not that there was a company behind, there was no state behind. What happened is that suddenly there was… The three things that you need to create Deepfakes. Tensorflow, so artificial in the machine learning algorithm was for free open source on the internet. The availability of personal data with faces on the internet was enormous. You could download alpha for Facebook, Instagram, whatever you wanted to do. The processing power that you need to train your algorithm was super cheap for the first time. And then all of this was put together by your community of people that did not even know each other. And in three weeks they create Deepfakes technology. And this is one of the biggest threat that you have to democracy these days. If you cannot trust and something that you said before, in terms of what deconstruct in between all people with internet is on the basis of trust.

If people cannot understand every day, the encryption, at least they need to trust that someone understands. They can trust that someone to safeguard their interest. And if suddenly you cannot trust what is presented to you via your screen, via whatever, that’s problematic. And there was no responsible behind. It is because, you were mentioning it before Patrice, the technology is moving so fast, and more importantly, the convergence of different technology is hitting and booming in a way that no one can really predict what is going to happen next. And for policymaker, this is siderating. They are like frozen. What I’m going to do. You’re telling me that what I learned is useless to what is going to happen because it’s exponential rise of technology. No one can plan exponentially. I know what happened the last five years, I can plan five years away, normally. Now the world doesn’t work like this. So it’s complicated.

□ And the politicians, you said they were freeze, they froze. How do you say in English ‘démissionner’?

/ Quit.

□ Yes, they have quit. They have quit long time ago. One of the interesting thing about the Internet, specially if you come with a background from France, French culture, French history, is that it is the first technology, which has been completely left to the private parties.

It was developed at some stage, of course, by the state: in the United States, in France, and in many other countries. But when it became really large scale, and I could observe that in the Netherlands, the government declined. Quit. That happened in the early 1990s, when we were doing in Amsterdam the Digital City, and we said, “Well, this is going to grow! We would need more government intervention and financing, of course.”And then, the government position was, “No, we are going to give it all to the private parties. Let the market lead the way.” And from there on, well… the rest is history in a certain sense. And that’s why I speak of this quitting of the government. And yes, you can spend a lot of time to explain to politicians and decision makers how it works. And so I am afraid this quitting deliberate, probably at an unconscious level, but as you say it’s too complicate, so we quit. And there’s something, again, we step now out of technology and go into general politics. That is a characteristic of the modern state. The modern state does not care anymore.

It does not want to handle these things. One of my many aside is that I’m a public transport interested person. Politicians would say, “We don’t want to get involved, it’s far too complicated for us so we don’t do it. Let the market do it.” And I mean, nobody forces you to take the tram. Of course, you have in Luxembourg, you have a fantastic system, but in general, it’s a kind of yeah… no.

When, in olden days, we were responsible for it and when it went well, we never got any compliment. When it worked badly, nasty questions in parliament. Now it’s easy. Are the trains not working well? The private companies are responsible. As you said, let’s look where are the responsible. Let’s search for the responsible, and let’s make sure it’s not us.

/ And it’s not impossible just to complement on this. Sometime policymaker, they can be ambitious. Sometimes they don’t know that they’re ambitious to be honest. Look at GDPR. This is a fact that at the very beginning of GDPR, the EU did not realize what it was going to do globally.

□ It just explained GDPR.

/ So GDPR is the General Data Protection Regulation, which is created from the EU. But in fact now pushes anyone processing personal data on the internet to set up some basic rules in order to protect the owner of this personal data. I mean, it’s kind of a shortcut, but that’s something like this. And because of something coming from EU, all the companies in the world had to change their processes, their business models, their notifications.

Okay. There’s another debate to say, is any of this effective or not. This we can discuss, but it really, changed the way companies had to do business. And on the basis of something that was purely ethical, it was about ethics. People needs to be in capacity to control their personal data. And now the EU is doing the Digital Service Act, which I think is going to have a similar effect because it’s on the content level.

So it's something about no content moderation, what can be on the platform, what cannot be right or recourse, take down of contents. It's and again, I mean, this content is not leaving somewhere. It's just passing by all over the cables of the internet.

✱ Yeah, I mean, I'm not, I don't want to justify anyone, but I just also think there are different speeds to these things. And technology is moving at a much faster pace than politics, pro articles or Democracy can keep up with. And also this idea of trust. I think that has been really exploited by big corporations that made a lot of money, like harvesting all of our data until someone told them, "Hey, wait a minute." You know, really telling us, trust us, we know what we are doing. And no one, maybe not even understanding really what was going on. I mean, the great majority of people then, of course.

/ And by the way, that someone saying, "Hey, what's going on?" That you're mentioning, he's a hacker. That's exactly what hacking is about. To me politically, it's investigative journalism, but hacker is in some sort an investigative journalist of the internet. You know, he is asking the question, pointing the fingers and saying, "Okay, what's happening here?"

□ With various consequences and a various degrees of success. And unfortunately, the balance is, there are some good developments, but I am myself a bit pessimistic because there have been in recent years major disclosures, which were of the caliber that you would say, "Well, no, now things are going to change." But there's a parallel with the COVID situation, which put a complete break on the economy. And suddenly people realized, well, we now have clean air and now pace of life has slowed down. Maybe we should really change. Well, at the moment, we are only a few percent lower than the emissions we did in 2019! So we are back to normal, quote/unquote. And with these disclosures, the last big one, it was not even the last one that had just come now, but I can't recall it exactly, but say the last one for me that was a really major break.

The major disclosure was Snowden. And that is why once Snowden had happened, I really got the kind of idea, that okay, "We have always thought it was like that, but now we know!" And there's really a difference between thinking where you are pretty sure… what is called in Dutch a probability, which is very, very, very close to certainty to the point of being absolutely sure of it. But now you are indeed absolutely sure. It's out, and things will change. Yet no, nothing changed. And it's even getting worse. So my question would be maybe it's kind of a turn to allow it or not allow this turn in the discussion: is maybe not time to put a break on technology? Or do we have to accept that, yeah, things are like they are. It's, I mean, do we have to live with it and do we have to live with Facebook till it dies itself? Or gets in the Metaverse, or can we not put a break to it? And that question is within the circles I am in a major discussion, and a bone of contention.

It is called de-growth or 'la decroissance' in French. And I am, just as I was in its time, a fervent advocate of free and open source software, 'and/or', I am now also an advocate for 'decroissance', for de-growth.

And de-growth means also technological de-growth, in the sense that you still can empower people in using technology to a far larger extent than you can now, and making it possible for them to use technology, to use IT. But at a lower level than the technology that we have, as it is being deployed and exploited by big corporation, and can be only by big corporation. So at some stage, I was very much into the discussion about Free WiFi. And Free WiFi, that means community owned and community run WiFi, and there have been a lot of initiatives. Well, they started as experiments and some are still ongoing.

One is in Denmark, one is in Catalonia and they work very well. People are connected. WiFi is functioning;. They have communication. But there's a little problem: YouTube is not going to make it through. Not enough bandwidth for it. So the question is: what do you want? What do you want, both as community, and as people? Or what do you want, as say, at government level? And at government level, I'm very afraid that in some instance, and it happens in the United States, they will actually forbid it. They will actually forbid non-commercial, meaning non-corporate, application of technology.

✱ Hmm. I wonder if there's an in between in this binary of de-growth, and the protocols that implement barriers or frontiers that try to regulate something that keeps molding and changing.

/ I don't pretend that I have the answer there, because it's a very, very fair question and a very complicated one. What I do know, is there's no way that regulation can technically regulate technology. This, I don't believe into it. We saw that, because technology is evolving in a way that no one even is in capacity to predict now, because of convergence and exponential growth. So this I don't believe in, technical limitation. A boundary in which technology is going to thrive, and it cannot go beyond this. That I don't believe it. But I do believe that regulators have a responsibility of at least promoting values, at minimum. It works, it doesn't work, history will tell, but their roles there is to protect the population on the values that are the cement of this democracy, of this state. Here I'm talking, democracy is EU, because this is where really you have this beacon of a bit of knowledge and hope, to be a bit ambitious on rules and regulations in the cyberspace.

So this should be pushed way more, being way more ambitious, and then from there you can assess if this is working or not. But at least to reach that point, because otherwise we are going to continue to say, "Oh, you know what, it's impossible." At the same time, no one is really going to try to stop it. So you're just going to boom exponentially, and you are going to have companies becoming the internet. And we're mentioning Facebook the whole time. In some part of the world, for them internet is Facebook, and tomorrow when the Metaverse is going to be out there, the internet is going to be the Metaverse.

□ Or it will fail.

/ Yeah, but you see what I mean. Same kind of logic here. The same way when they wanted to send their own currency, and then suddenly...

Let's take the example of Libra. So when Facebook wanted to put Libra out there, it's an interesting one, because they could secure partnership with quite big financial companies. So they had this backup of the industry, and then they hit a hiccup that they haven't seen coming. Because Facebook, anything can go. It's that states woke up and said, "Wait, wait, wait, wait. Isn't that the sole role of state, to create money?" And that's very interesting, because at the same time cryptocurrencies were out. Except that with crypto, there's no state behind. There's no Facebook behind. There's no entity behind, so you cannot really say, "Who is behind making Bitcoin and Ethereum?" It's the community, so it's very difficult to regulate. And then suddenly there was a face. There was a name that was going to create money outside of state, and then suddenly states woke up.

So it's not absolutely impossible. Yeah. I would say, ambitious regulation and reading the world today, it's EU should lead. Sadly enough, it looks like EU is not in the strength to lead and that's not great, because otherwise something that we discussed about since the beginning, hacking. For hacking to exist and to work, it's deeply linked to the existing infrastructure of the internet. How the internet works. There's now as we speak, initiative from states, to change the deeper nature of the internet to transform this into a centralized system controlled by states. And it's not a hypothesis that it could be 10 years ago, 15 years ago. People are saying, "No. It's impossible. They will never change. They want to do this technique, it is impossible." It is very possible, and if that happens then this is the root of everything else. Then you change how people connect with each other.

□ Well it's funny, because at that stage where the states, according to you and I agree with you, was the stage in the very beginning of the internet. And ITU, the International Telecommunication Union, wanted to keep control and failed to keep control. It failed to keep control, I think, because of passive or active U.S. Government intervention which wanted to keep the Internet American. But the funny thing is that in those days, we people who were for a free Internet, objectively were supporting the US Government and ICANN in this. And now we are back to it. I think what you just described made me think, "Okay. That is plan A." Plan A is as you say, the European Union kicking into action and doing something. Do we have a plan B?

/ We are living plan B. That's the problem. We are in plan B every day, because no one has the ambition to do a plan A, plan AB, plan whatever. There's no plan.

□ Okay. Let's call plan C, that is. What is plan C?

/ Yeah. True.

□ Plan C, would be that people take power. That the users would be also the producers. Well, I call them the producer, but what I want to say is that the things are owned and run, and if possible, also developed by the people. And no, not if possible, but necessarily, it will have to be developed by the community, by the people. Is there any chance to that?

/ But which means that you need states to invest into digital literacy for their population. You need states to trust their people, and to give them a lot of knowledge so that they can become really these digital citizens. Enlightened, understanding the technology and with the capacity to self critically decide, "I'm using this app. I'm not using that one. In fact, I'm using no apps, because I don't need apps and I can go back to the structure of the internet." But this is an effort of states. Providing a lot of knowledge for citizen to become something else then consumers.

□ That will kill the business model of corporates!

✱ Yeah. Because I think these values that maybe you are talking about, they're not shared. And when you talk about the free internet and an open system, I think that was an idea that has been completely lost. And if internet was ever a public space, now it's a completely private one, and I think also people engage as individuals. Like, community spaces are no longer there, so I think it really requires a whole new system.

/ And it's also nuance, I guess, because you cannot hope that state is going to be responsible for the old stack, up to the application, down to the technologies. The private sector will always have a role there. Just a question of ... Okay, I'm not talking about the de-growth option. I'm talking about, there's a regulation. There's a clear empowerment of people to understand what they do and understand the ecosystem, becoming empowered. But there's still, I guess, an industry behind that is providing some tools or others, because not everyone will be in capacity, or having the time or the appetite to develop their own tools, to be within the open source. We saw that. But these companies can really well, and they show that they could be that rule with GDPR, go back to GDPR. Could really well operate in a framework that will be properly regulated. Now the problem is that this is not there. It's self-regulation. There's so much call for self-regulation. We saw what self-regulation was doing in the financial crisis. It's what you're mentioning.

□ Well, that has a lot to do with the problem, and I completely agree with you, the kind of companies who could do that will by definition not be big, monopolistic companies. They will be small, community, local companies federating, so sharing the knowledge. Not so that everyone develops the wheel or reinvent the wheel in it. But you were using the word 'private'. Maybe private has a good connotation and refers to individuals. I think, as a kind of discussion proposal, it is better to always use the word corporate. It is not about public vs private, it is about public vs corporate. And the regulation you are proposing is so much against the interests of corporates, that, also given the osmosis, often at the personal level, between government and corporates, I am not very hopeful about that.

/ No, no. I'm not saying something to happen tomorrow. No, for sure. For sure.

□ How can we make it happen? I'm not demanding an answer!

/ No, no, no. No, no, no. I get that. We go back to trust.

First, we go back to staying ambitious. And there was a report yesterday in Switzerland, from the National Center for Cybercrime, about the fact that crime is on the rise. Cybercrime etc., everything is bad. And yeah, factually speaking, it's worse than it was, but it's exactly the time not to be, "Oh, okay. Nothing works. What are we going to do?" In the contrary, and I was thinking about the situation, to be honest all the tools are there. That's the worst. That's the worst. The tools are there.

It's just that they're not used, because again, and I'm pushing a lot of responsibility on states, corporation have a lot of responsibility too, but in this case it's states. States are there to lead the way and to say that, "All the tools that we have, at least let's use them to the bone, and then if they don't work, then we see if we need something else." You were mentioning this speed of technology, etc. We're saying that, criminality and abuse are evolving at the speed of light, and we are not even replying at the speed of law. We have laws. We're not even there, so what?

□ Now, if you say that, but I hope I'm not sliding down into the conspiracy this way, but when you say that, the impression gains ground, that somewhere it is deliberate. And that 'deliberate', I will always say is not at the conscious level, but at the unconscious level. It is somewhere in the DNA of political power. We were discussing power coming in and out. That's interesting, and maybe we have to come back to that. But before coming back to that, I would talk about trust, because trust is indeed so essential, but at the moment in what kind of system are we living? We are living, in fact, in a trustless system. And why? Because the impression has gained ground that trust, which is a basically human thing… It's maybe not a thing, it is an essential human characteristic, and because of that trust cannot be trusted.

And we have walked into a situation of trustlessness, which is in a world of machines. And that has a very long history. And that history, one of the author, to me, who has explained it best is Manuel De Landa, in a book which is called, *War in the Age of Intelligent Machines*. In that book, Manuel De Landa, explains that very early on, in the United States, during the say, 'structuration' of the United States, in the years after the War of Independence, so we are talking first half of the 19th century, the idea gained ground that when you had a chain of decisions making, of processes, the weakest element in the chain was always the human. And this human had to be taken out of the chain and replaced by protocols, by fixed rules. And nowadays these protocols and rules are enforced by machines.

And then you get a whole situation that the trust is taken out of the system, and it is a basic philosophy of cryptocurrencies. It is to take the human out and replace it by what I would call, well, not me alone but many people will call it, algorithmic trust. You don't need to trust humans, because the protocols enforced by the machines will do the work. Once you are into that, you are also out of political decision making. So if you have a system like ours now, where a lot of things… look around you, it's not only technological. A lot of things are based on pre-established rules and post-happening certification. To me, by then, you are lost. And I have seen this in so many times.

I was academic, but I was a kind of ‘maverick academic’, because I never went into all kind of things. One of an academic thing, establishing the credential of an academic, is a CV. Well I never had a proper CV. I don’t have a bio! I don’t have a record of what I wrote. I don’t know what I wrote. But it doesn’t any longer work like that. It did work in the time that you had human trust, because people knew you and that was sufficient. I’m sorry if I’m talking in all kinds of directions. I see you frowning.

/ No, no, no. I’m with you. I’m with you. I’m with you. I’m with you.

✱ Yeah. I’m there too.

□ In the olden days, to obtain a passport in Great Britain the only thing you had to do was to provide a photograph, and have that photograph signed by your local member of parliament. You went to your local member of parliament’ surgery, to his speak hour. And it went like, “Oh yeah. Oh yeah. You’re Mr. Smith. Yeah. Yeah. Fine. Oh yeah. Okay. Okay. Sign here. Sign here.” And you sent the application form and photograph to the passport office, you got your passport. And why? Because there was trust, and it worked. That’s a fantastic thing in my mind.

And another example, which really, I think this is a very good example of how human trust and honesty works, ethics. Is that in the High Court of Scotland, all judges had a pigeon hole where the lawyers of the conflicting parties put their brief, their arguments, what they are going to say to the judge. So in the same pigeon hole, reachable from outside, you have the argument of party A, and party B. Now you immediately understand that party B would really much like to know what party A is going to say. Well, the lawyers of both parties would not even think of taking it out and looking at. And that is a form of trust that has disappeared nowadays.

✱ But I guess also, because you take the human out the way-

□ Because you take the human out. Yeah.

✱ So I don’t think you can apply the word ‘trust’ to algorithms. I think it’s a cop out. People don’t trust algorithms, they just let them do their thing and never question them. So I think philosophically, we have to go back to the idea of ethics and responsibility that you can only apply to people, or people that take on that. I don’t know if you agree.

/ Yeah, I do. Just reflecting on what you’re saying, if you put trust and algorithm in the same conversation, and how it relates to hacking and understanding the system. I go back to hacking for understanding the system, how it works for the sake of improvement or the common good. If we consider that algorithm replaced law. Because when you code some rules that gives you an environment, you can only operate in these rules, and this rules are managed by an algorithm. Defacto, this algorithm is the law.

□ Yeah. Code is law. That's a famous book by Lawrence... Lawrence, not Lang, but the other.

/ I don't remember.

□ The person who wrote about Creative Commons, CC.

/ I don't remember. But that's the idea, suddenly it becomes the law. If you don't have hacking activities to scrutinize this algorithm, to understand how it works, to look into the core of the algorithm, then there's no bias because the algorithm at the end of the day is not coded by machines. Even if that one was coded by a machine, before that one it had been coded by human at some point, and on the basis of decision making that was human related. So it's not that because you put human out of the loop, that human was really out of the loop. There was something somewhere. And we saw the scandal with face recognition not so long ago, in terms of the facial recognition algorithm. It was more in capacity to recognize a white male rather than a white female. And it was between white female and black female, then it was absolutely no down. Why? Because the bias, because of the dust of the sources. So hacking, again, looking in the codes, understanding how it works, why it works.

An anecdote. A student, I don't remember where. They were learning, machine learning, so training machine learning algorithm. And they were trying to have an algorithm which would automatically detect a banana. So when they would put a banana in the frame, it would detect the banana. People are not very... Hair, bald, I don't know. What can I tell you? And that was very funny. So they were taking the video, they were putting the banana, and then as fast as possible it would detect it and giving them a light or whatever. And then it became super, super fast. And then they tried to look into the black box of the machine learning so you know what works. And they saw a neuron in the middle of the black box that was super active, and it looked like it was very effective. And why? Because it became a face recognition algorithm. A face detection algorithm, because the machine learning program quickly understood that when the face was coming in, the banana was coming just afterwards. So it became very good in working in that face, but if you don't know how it's coded you really think it's working on the banana. No! It's working on the face.

* The noises you might be hearing is us having some chocolates. And we are here in a bunker, and I'm sitting across from Patrice, that is wearing an amazing purple T-shirt that says 'Vatican Hacked Embassy'. Maybe he wants to tell us something about that.

□ The people cannot see the T-shirt and T-shirt is very special. There are not many of them, but told very quickly, it is a story about the big hacker events where I used to go. Well, even earlier I used to co-organize them, and they have become so big that people organize in 'villages' of mind alike folks. Some people are all coming from certain countries, and then it is called an embassy. A friend of mine was a long time part of the Italian Embassy, but he got kicked out of the Italian Embassy.

So he started his own which was the Vatican Embassy. But Vatican Embassy, that is a bit bizarre, so he put in ‘hacked’ in Vatican Hacked Embassy, and he still went to these big Chaos Computer Club, German Hackers Organization events with this T-shirt, and bringing along better quality grappa than his Italian ex-friend who had kicked him out. That’s the story of the T-shirt.

✱ To give you a funny interlude I remembered a book by an art critic from the U.S., called David Hickey, that is titled *Pirates and Farmers*. And I remember one of the words Lara’s list mentioned was pirate. Again I guess, in relationship to this weird idea of hackers. So David Hickey writes:

“I’m going to explain this to you very simply. All human creatures are divided into two groups. There are pirates and there are farmers. Farmers build fences and control territory. Pirates tear down fences and cross borders. There are good pirates and bad pirates, good farmers and bad farmers, but there are only pirates and farmers. They are very different kinds of creatures, and some pirates even recognize the importance of farmers. My late friend, Roger Miller, a famous pirate, wrote this in a song after a visit with his tax attorney. “Squares make the word go around,’ he wrote. ‘Sounds profane, sounds profound/ but Government things can’t be made do/by hipster wearing rope-soled shoes.” Dave Hickey, Pirates and Farmers (London, Ridinghouse, 2013) 17

□ That’s a nice one. But it’s interesting that he makes a distinction between pirates and farmers, because the classical anthropological distinction is between nomads and farmers. And the problem is exactly the same, in sense that pirates are nomads of the sea. And now we really move out of IT, but back into capitalism in a certain sense. David Graeber, who as an anarchist anthropologist is very famous for his book *5,000 Years of Debt*, which is really a fundamental book, wrote, and it is not very well known, also about pirates. Pirates are seen, in a certain sense, like the same way as hackers, as representatives of democracy, horizontalism, sharing, knowledge seeking. And he is not the only one writing in that sense about pirates, because, like in many things in history, there are some accepted opinion about other period of times. A nice one example is about the dark ages. And as group, a nice one are pirates or there are also Templars, and ... Well, quite a lot of groups to which the mainstream has attributed generally a bad opinion to. But there’s contrarian opinion often backed by, if not facts, at least good evidence, that it can be seen differently. And then you get a conflict between people holding for, I mean among the specialists, holding for the old opinion, and others holding for the new opinion. And Graeber, whose last book, not his last published book, his last unpublished book, that means not published in English language, but translated and published in Italian and in French, is about ‘Libertalia’.

It is the story of pirates on the coast of Madagascar, the West Coast or is it the East Coast? No, yeah, the East Coast of Madagascar at the very end of the 17th, very beginning of the 18th century. Having escaped the Caribbean, because the Caribbean had become really pacified by mainstream powers.

And restarting their allegedly very democratic, very horizontal, very sharing communities on the coast of Madagascar. Graeber got being attacked by other specialists on pirates, as someone projecting ideas of the 21st century into the history. Whereas everyone knows, at least they knew, that pirates are really bad, and their societies were extremely cruel and extremely unequal and extremely aggressive, also among themselves. And this utopianism was absolutely out of bounds. And the same kind of stories you have about nomads and farmers, or in the United States about cowboys and Indians.

What's the mainstream idea of Indians? Well, it's not very good. They're are very cruel culture. What is the 'revisionist' story about Indians? It is that they are very good people and very close to nature and actually are pointing to our future. And so you have so many examples, and well you have about the hacker story, you have exactly the same.

* Yeah. Do you have any pirate stories for us?

/ It reminded me the fact that... I mean, at least I remember this for my courses of history, about French history. When there was still a king in France, he was using a 'corsairs'. So pirates, specific format of pirates, which were allowed by the king to go out and ransom, rampage, steal, you name it. But it was covered, because ordered. But at the same time on their free days, they could also do some pirating for their own intent and their own.

The same is happening now. I mean, you have criminal groups that are working very close to state interests, or if they don't work close to state interest, at least state let them consciously operate. So it doesn't mean that they are accomplice, but at least they are clearly a, "I close my eyes into what you're doing. As long as you don't take me or my interest." And it's a situation that reminds me what we could see in this old age and the word pirate. Yeah. Rang that now.

□ I think it's a very good comparison. And then we get into states, deliberately engaging into activities which endanger the... well, it endangers the Internet, it endangers the people which become very vulnerable and indeed these people having also sidelines in, I would think mostly, in the ransomware department.

/ Yeah. There's ransomware. There's all these department. I mean, but something you just said, and just to be clear it's not the only place where I would voice it. But I think it is critical point is that, the insecurity on the internet is the responsibility of states. And not only of states because of regulation, etc. I'm talking about attacks. I'm talking about being behind attacks or letting attacks go. The responsibility of states is still not that guy in the hoodie, in his garage or in her garage. No, that's not the corporate, it is the state. When you see attacks on the scale of SolarWinds or you see this market of surveillance that is not only allowed by states, but is purchased by states. You have companies like NSO putting this malware like Pegasus, where you can transform the phone of anyone in zero click into a portable spy. This exists because these companies are not hiding.

They're not in the dark net somewhere. No, no, no, no, no. They have a building in the city. Everyone knows them. They spend million in research and developments and each and every dollar, euro, penny that is sent there, is against the internet. Because it's to find holes in the internet and to exploit them against or common interest. And these companies exist because states let them exist, first. Second, buy them product. And third do not regulate how this product are exported in between states. So this is the highest level of responsibility. Then we can talk about this script kiddie that is playing with the network of the library, the next door. Okay, we can talk about this, but let's have a bit of a-

□ Well, in Italy you had 'Hacking Team'. We have a few more, but… I was thinking about something, which as usual or as happens, I got lost into and yeah-

/ I mean, to reply to the hacking team that's because we're starting with that word. It's good to go back to it every time. Hacking team was an abuse of the word. I mean, hacking team has nothing to do with hacking. So I mean, it's not because you claim the word that it means that this is activity that you're doing. They were just taking money to exploit vulnerability in the internet and to empower mass surveillance, that in lot of cases was going against human rights.

□ With the states, which were their principal clients and the states should have, in this case, the Italian state should have regulated them in selling. And that is what they pretend they did. And all these companies are pretending, "No, we sell only to legitimate parties, democratic states for purposes of combating criminality." And, yeah, then in the end, it turns out that they sell to dictatorial regimes, going after human right activists.

/ Yeah, and who knows what the state is going to become tomorrow. I mean, you sell to a state today and you think that this state is democratic, and incidentally something happens. And then-

□ It happens in our own time! I'm very glad that you are saying this because it reminds me something that again, pre-technology, or pre IT as we know it. It was a time of Tony Blair who was prime minister of Great Britain, of the United Kingdom. First Tony Blair and then his successor, Brown. Which is-

* Gordon.

□ Yes, Gordon Brown implemented extremely liberty-threatening laws. There were attacked on that. Well, the opposition was saying, "But these are liberties-threatening laws! A yeah, but we will only make good use them. It will be only in the defense of democracy and the legitimate rule of law and order." But when someone said that, "Yes, but you never know what can happen, even Great Britain can become a dictatorship." Actually, there is a very good television program of the BBC, which ran 20 years ago or more. And then was shelved because too dangerous, too bad to think about it.

Where you saw extremely credible scenario of government being elected into power which was really not in the interest of-

✱ What was this program you're mentioning?

□ Yeah. Well, I'm trying to remember. I can better describe it. The idea was a Labour-like, popular politician became elected prime minister. Well, election gave him a sufficient majority in parliament to govern. And he was implementing... this new prime minister was implementing policy, which were clearly not in the interest of the power that be. And these were policies of economic, but also political, and would almost say cultural interest. And he was toppled by an intervention, which portrayed his government as causing a situation which was endangering the existence of the state. And there was a kind of silent coup and then things came back to normal. I can't even remember if he was assassinated or not, or whatever what. In any case the whole idea was that a democratic government could be overturned in a fairly efficient, not-too-bloody manner. And then you can get the government, you can get an extremely repressive government having all the surveillance tools. And that is what we have seen in the United States far more recently with Donald Trump. I mean, it's a complete nightmare. If the guy comes back. I tend to think he will not, but okay. Donald Trump was well on his way of implementing a completely different order in the United States. Backed up by instruments of surveillance and control and repression. Which are incredibly effective and no longer resistible. I mean, that's also a thing of technology. Quite often, you have the thing that, "Oh, if the Stasi only had the surveillance capacity that we have nowadays the whole system would still be there." An optimist will say, "No, there's this psalm which says empire raise and fall. Everything that raises will come down." But meanwhile, it's quite frightening, it is a quite frightening prospect.

/ What about art, in all of this?

□ Yeah. What about art?

✱ Well this exhibition, that it's on now here at Mudam, tries to tackle these complexities. And I think it's really hard for people working with materials and ideas, to be able to compress this so much into a sculpture or a video, or installation, whatever it may be. What I'm asking myself is in this kind of political ecology, I think we talk a lot about interest, commerce and financialization. That it's led by capitalism and by corporations, but I'm also personally very worried by the role culture doesn't play into this. And it's quite interesting if you analyze a bit, also how like Silicon Valley has been moving along. I think culture has really been one of the places they colonized quite early on. Say with the project of Google archiving, owning the rights of all these artworks, with the idea that you could pixel by pixel experience them on your computer.

But at the same time acquiring the possibility, the same with Bill Gates owning the Getty Images. And I think also about the paywall established around universities, or academic papers, this idea of inaccessibility and yeah, kind of closing off rather than making shared. Because everything needs to be a profit.

I don't know if you have any take on this. Because I think culture is a bit always what is missing in this conversation, because it's easy to go to the technology or the effects.

And also it's what is missing in political discussions. I mean, I'm taking the example of Italy with the lockdown. They invested a lot of money to restart the economy. And of course, there were huge problems in a lot of areas of being, what was perceived. And it was the most impressing issue, but culture was always forgotten, was not there or was the very last step.

/ Same in France-

* And I think this is a big problem. And I think empowerment to me means also, having more access to information and culture or the right to culture, is a big part of that.

/ Now art is... I mean, there's something unique about art, when it comes to these topics is that you can... There's the capacity for artists to give a story about the cyberspace with all these new ones. Doesn't have to be pro-technology, anti-technology, art it can transcend that. It can project to you into one single piece of art, the complexity, the paradoxes, your position and you can really... So I'm always very interested in when artists are taking, they're embracing this complex topic of cyber ethics, what this means for knowledge, what this means for the future of the generation and trying to vehicle a message. So, that's why I was asking.

* Yeah. And I think maybe what's interesting in how artists approach this, is that they don't represent anyone but themselves. So they can really see through very different lenses and with their research going very different directions. So maybe that's what... Is like infiltrating spaces that are-

/ Last year we had an event, it was November last year, for the first year of the institute. And we invited artists to produce some artworks asking what is Cyber-Peace for them, what does it mean? It was mind blowing. Because you work on this every day, but you work on this under the lens of, "Okay, this is about attacks, about victims, about laws, about norms." So, it's kind of super framed in my mind. And then someone comes say, "Okay, what do you think."

* I'm generalizing and maybe romanticizing this a bit, but I think art has always had this capacity of imagining futures. And maybe the answer is somewhere there, or at least they can prospect things that are not on the horizon yet just with their... And I think a lot of also the cracks, the problems, as you were saying, like the bias attached algorithm, because they come from humans, from intentions. I think there's really interesting artists developing work about that now, like in the exhibition, Martine Syms and Sondra Perry. How algorithm disregard black female bodies and how to take back that space and like turn Siri or Alexa into a different kind of space.

□ I would even top up on that. I think that at the moment the artists are the last ones which are going quite far in understanding the whole issue, and are able to portray it. There's a book which is called *The Great Offshore*, we talked earlier about it, which was done by The Rybn Collective, which is entirely written by artists. And they have really explained the phenomenon far better than any academics I know the economics working of the situation we are now at the moment. *The Great Offshore* is about capitalism outsourcing itself in various location, like what we've known as tax paradises and so. And it is quite fantastic and there are many instances of that. And the reason why you were saying, is that there are independent, they are not involved. They are not, how you call it?

* They don't have a specific agenda.

□ Yeah, a specific agenda. But this is ... you should watch out because this is changing, also the whole artistic cultural field is now falling prey under this, what I call the certification mechanism. And the authorization thing that also artists are going to be framed, are going to be enclosed in the system. I see it in, for instance in the Netherlands, in two fields that artists are encouraged, and you should read for encouraged more or less forced or nudged as it is, to go for a PhD which is the absolute example of a certification paper on one hand, and on the other hand to behave like entrepreneurs. So to become cultural entrepreneurs as it is called. Which is a way to include them in the monetary capitalist system.

But for the moment as far as I know, they are resisting. And when I was in academia, I was noticing that theory was going out of academia in favor of basically, in money bringing in practical projects in the field of development, 'development' again, between brackets. In which this was, to me, very obvious because the department was basically functioning as a knowledge resource base for the Ministry of Foreign Affairs and of development aid. And theory was going out, critical theory of development in this case, was going out. But theory was moving to art schools because they were still independent, they were still out outside the system. I don't know if it's still the case. I'm very afraid that if you go to an art school this day, that they will say, "Oh no, no, this kind of field is no longer financed. It's no longer supported."

* Well, I mean, it's been a while also for me, but I sympathize with what you're saying. Because when I was studying in London, I went to Goldsmiths, which prides itself as being a hotbed for theory and thinkers. And it was quite interesting because they kind of really cherish their independence. And what happened as a student, you have this kind of badge of honor that you graduated from there, but then you're on your own.

And then the colleagues from the other schools, that are much more connected to institutions, they were the one getting the jobs or the internships. So there's also that reality. And I think art is always been infiltrating spaces that are borderless. But even in the '60s, in the UK, there was the Artist Placement Group and they were going into factories and learning or making the other forget about the Taylorist way of production.

□ Yeah, yeah yeah yeah!

* And nowadays Silicon Valley does residencies for artists and artists go there. Because they probably get five times the money they would get from a residency in a museum or an institution, and the access tools in a different way. So it's a very complex world to navigate, as pirates or farmers-

/ I think we covered quite some ground. It's 5:43 PM now-

□ And there's still so much ground to be covered! There are so many things to be discussed, but-

/ Nice conversation. Very nice.

* Yeah. So everyone agrees? So we-

□ Maybe I can plug something because you were quite at the beginning talking in terms of empowering people and that's what your institution is doing. There are many more institutions doing that, fortunately. I hope you also federate and know about each other. I was for instance, with the Tactical Technology Collective, which started as... well, that was when I was advocate for Free and/or Open Source software, as I called it. And there's a group in Italy, which is called C.I.R.C.E, which is doing exactly that. They are giving classes to people, you know them?

/ Yes, I know this one.

□ You know this one. But you know the group as well?

/ The group, no, no. I know the book.

□ And it's all about going to the people, going to classes in schools, and explaining how technology work and telling kids, 14 years old kids, "Okay, you have a smartphone, do you know how it works? Well, it does this, this and that. And if you do this, this and that happens. And you don't use apps? Well, yeah. Maybe some apps you can maybe use, but maybe others less so because this, this and that is happening then". And it's... Yeah, that-

* And for the listeners out there, the book is Agnese Trocchi *Internet, Mon Amour. Chronicles Before Yesterday's Collapse.* And there's a heart on the cover, a heart that it's technological in scope, I guess.

□ Yeah. That's empowering, making people attaining technological sovereignty. That's the bit, that's is our hope.

/ It takes time, but it takes also willingness and, again, ambition from education program and everyone around school that wants to have...

In another life, I wrote a play for that, that was played a lot in schools in fact. To give like a ready hands on story about what is happening when you just let go, when you let technology drives everything and then you just let go, and it works with kids. You always think that there's no interest, privacy is a value that they don't believe in anymore, whatever. It's not true at all. It's even the contrary. I mean, it's quite... I guess there's this kind of misunderstanding about the millennials and the Z-Generation, whatever it's called now, that they are like... Because the digital natives, they understand digital. It's absolutely untrue, is very wrong. They have been raised to be in fact manipulated by digital means and without really taking the time understanding how it works, but it doesn't mean that they don't have the capacity to... or the couragity to understand how it works.

□ Well, they've been raised as consumers. But you can make them producers. And you can make them producers, not by imposing programs, by imposing curricula. But so you can make them producers by explaining and by being an example and by facilitating them. And so I'm... Yeah-

/ Especially because you see there's the... Sometimes the meme, the meme generation makes me think about this. It's kind of hacking of the content. It's like there's a content that is passing by and you have this glimpse of joke and smartness, to transform this content into something super fast, super fun for the whole community. Then what was originally content is transformed into something else. And then it gets a distance to understand that. So then suddenly people get a distance in what is presenting to them. So it shows a bit of self criticism also. And so, it's there, it's really there. We should not mistake this generation to be blind consumer, but as long as that, an ambition to make them like really inform consumer and to help them.

□ Exactly.

/ What can you hope?

□ Is there a password for us to escape? Or how does it work?

* I don't know. Get us out of the bunker!!